访问web页面过程:

1）DNS解析过程

2）HTTP请求响应过程

编写网络嗅探器的流程

1）打开设备（libpcap open）

2）设置过滤器

3）For循环：

a）抓取报文

b）报文解析

1）打开设备（libpcap open, libnet open）

2）设置过滤器

3）For循环：

a）抓取报文

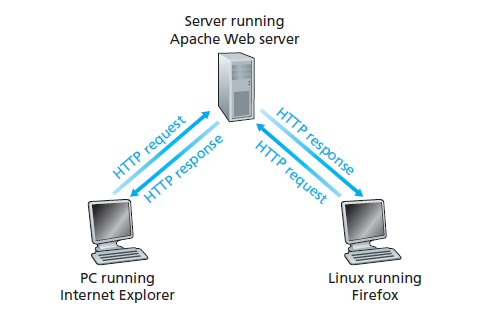
b）报文解析

c）内容匹配

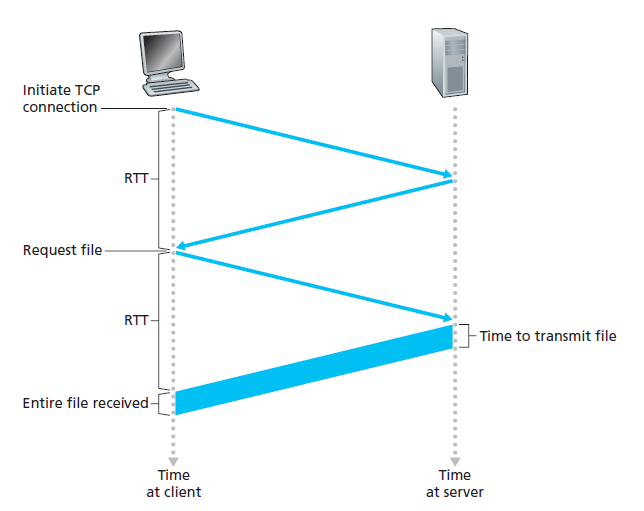
d）伪造响应报文

e）发送响应报文

HTTP的请求-响应行为：



请求并接收一个HTML文件所需的时间估算



典型的HTTP请求报文：

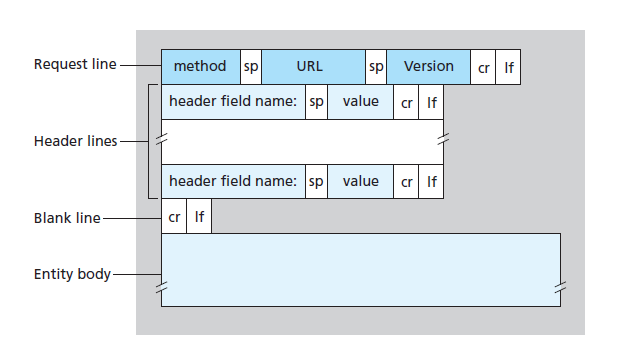
GET /somedir/page.html HTTP/1.1

Host: www.someschool.edu

Connection: close

User-agent: Mozilla/5.0

Accept-language: fr



HTTP/1.1 200 OK

Connection: close

Date: Tue, 09 Aug 2011 15:44:04 GMT

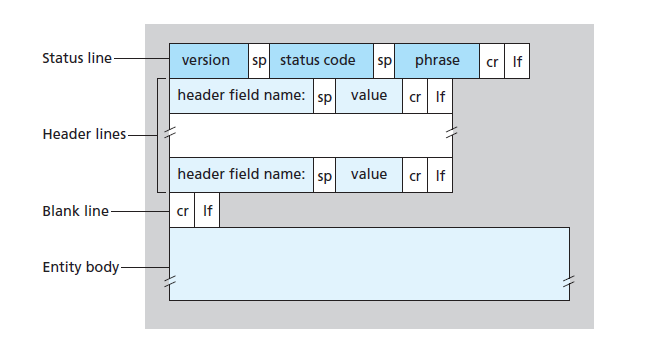
Server: Apache/2.2.3 (CentOS)

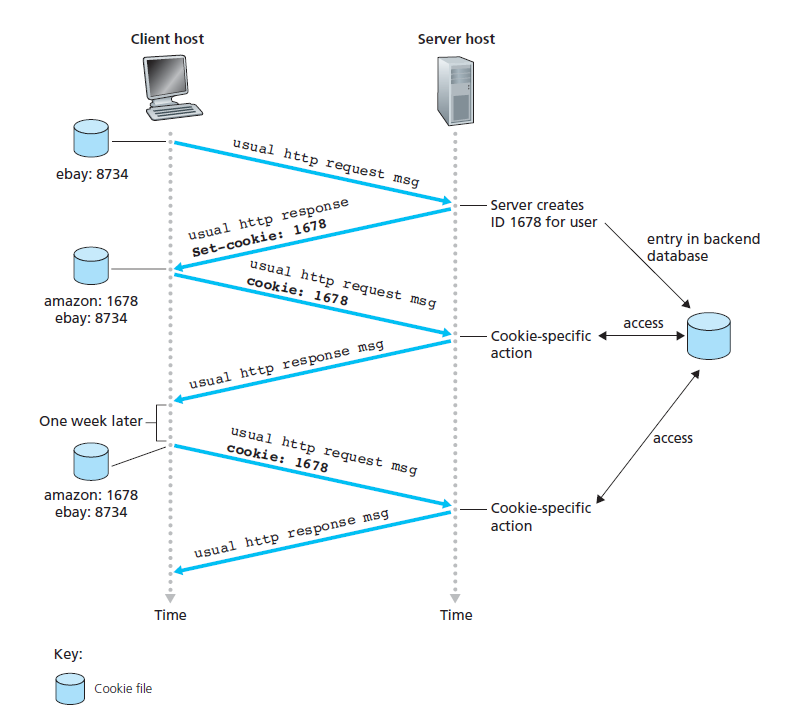
Last-Modified: Tue, 09 Aug 2011 15:11:03 GMT

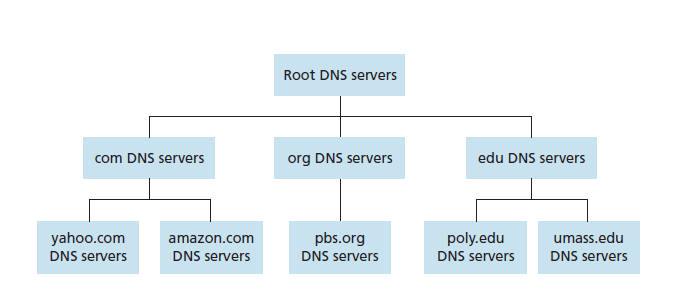
Content-Length: 6821

Content-Type: text/html

(datadatadatadatadata ...)

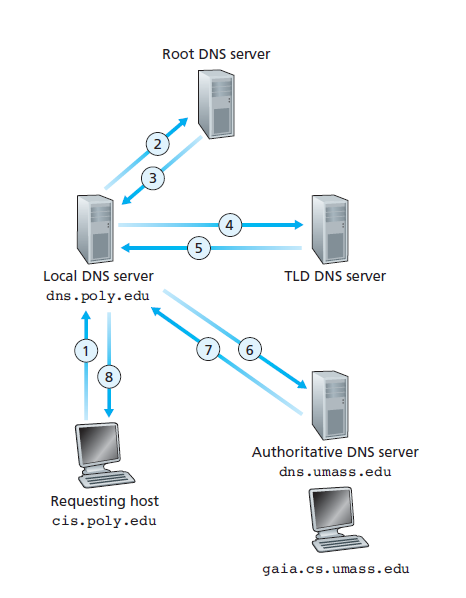






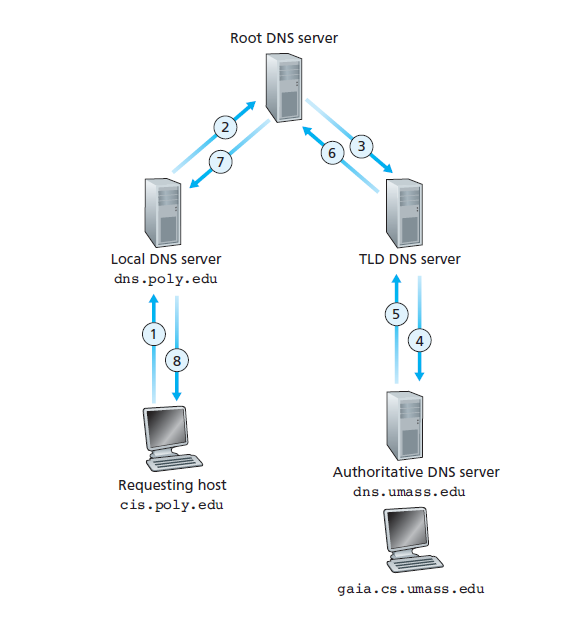
DNS服务实现方式：分布式、层次数据库。

DNS分类：根DNS服务器，顶级域DNS服务器，权威DNS服务器。本地DNS服务器，每个ISP都有一台本地DNS服务器。

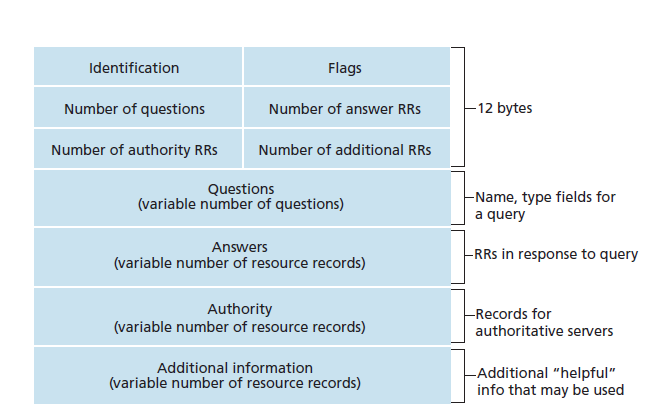


一个简单的域名查找过程：cis.poly.edu访问gaia.cs.umass.edu。

DNS查询方式：递归查询和迭代查询（cis.poly.edu到dns.poly.edu是递归查询），后继3个查询是迭代查询。任何DNS查询既可以是迭代的也可以是递归的。



一个完全的递归式的查询。



DNS报文格式。